

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-186546

(43)Date of publication of application : 16.07.1996

(51)Int.Cl. H04H 1/00  
 G09C 1/00  
 H04L 9/18  
 H04N 7/167

(21)Application number : 06-328027

(71)Applicant : SONY CORP

(22)Date of filing : 28.12.1994

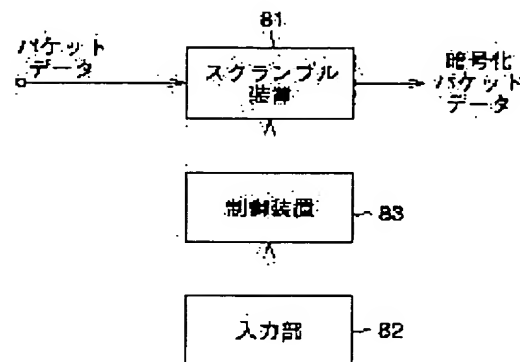
(72)Inventor : YAMASHITA MASAMI

## (54) SYSTEM AND METHOD FOR SCRAMBLE AND SYSTEM AND METHOD FOR DESCRAMBLE

## (57)Abstract:

PURPOSE: To provide information in a state rich in changes.

CONSTITUTION: A control circuit 83 controls a scrambler 81 corresponding to an input from an input part 82 and scrambles video data or audio data for the unit of a packet. In a first mode, only the video data are scrambled, in a second mode, only the audio data are scrambled, in a third mode, both the video data and audio data are scrambled and in a fourth mode, the video data and the audio data are respectively alternately scrambled.



## LEGAL STATUS

[Date of request for examination]	05.07.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	abandonment
[Date of final disposal for application]	25.01.2005
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

**THIS PAGE BLANK (USPTO)**

**THIS PAGE BLANK (USPTO)**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-186546

(43) 公開日 平成8年(1996)7月16日

(51) Int. Cl.

識別記号

F I

H04H 1/00

F

H

G09C 1/00

7259-5J

H04L 9/02

B

H04N 7/167

審査請求 未請求 請求項の数 6 O L (全13頁) 最終頁に続く

(21) 出願番号 特願平6-328027

(22) 出願日 平成6年(1994)12月28日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 山下 雅美

東京都品川区北品川6丁目7番35号 ソニー株式会社内

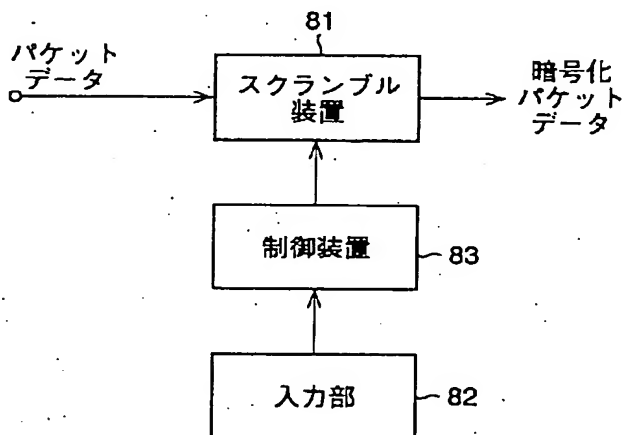
(74) 代理人 弁理士 稲本 義雄

(54) 【発明の名称】 スクランブルシステムおよび方法並びにデスクランブルシステムおよび方法

(57) 【要約】

【目的】 変化に富んだ状態で情報を提供できるようにする。

【構成】 入力部82からの入力に対応して制御回路83はスクランブル装置81を制御し、バケット単位でビデオデータまたはオーディオデータをスクランブルする。第1のモードのときビデオデータだけを、第2のモードのときオーディオデータだけを、第3のモードのときビデオデータとオーディオデータの両方を、第4のモードのときビデオデータとオーディオデータを交互に、それぞれスクランブルする。



## 【特許請求の範囲】

【請求項 1】 パケットを単位として伝送するビデオデータとオーディオデータの少なくとも一方を、前記パケットを単位としてスクランブルするスクランブル装置において、

前記パケットに含まれるデータが、前記ビデオデータまたはオーディオデータであることを表す ID を検出する検出手段と、

前記ビデオデータをスクランブルする第 1 のモード、前記オーディオデータをスクランブルする第 2 のモード、前記ビデオデータとオーディオデータの両方を同時にスクランブルする第 3 のモード、前記ビデオデータとオーディオデータを選択的にスクランブルする第 4 のモードのうちの少なくとも 2 つのモードの 1 つを選択的に設定する設定手段と、

類似ランダム系列を発生する発生手段と、

前記発生手段の出力する前記類似ランダム系列を前記ビデオデータまたはオーディオデータに加算する加算手段と、

前記設定手段により設定された前記モードと、前記検出手段により検出された前記 ID に対応して、前記類似ランダム系列の前記加算手段への供給を制御する制御手段とを備えることを特徴とするスクランブルシステム。

【請求項 2】 前記類似ランダム系列を生成するための初期値を、前記検出手段により検出された前記 ID に対応して修整する修整手段をさらに備えることを特徴とする請求項 1 に記載のスクランブルシステム。

【請求項 3】 パケットを単位として伝送されるとともに、前記パケットを単位としてスクランブルされているビデオデータとオーディオデータの少なくとも一方をデスクランブルするデスクランブル装置において、

前記パケットに含まれるデータが、前記ビデオデータまたはオーディオデータであることを表す ID を検出する検出手段と、

前記ビデオデータをデスクランブルする第 1 のモード、前記オーディオデータをデスクランブルする第 2 のモード、前記ビデオデータとオーディオデータの両方を同時にデスクランブルする第 3 のモード、前記ビデオデータとオーディオデータを選択的にデスクランブルする第 4 のモードのうちの少なくとも 2 つのモードの 1 つを選択的に設定する設定手段と、

類似ランダム系列を発生する発生手段と、

前記発生手段の出力する前記類似ランダム系列を前記ビデオデータまたはオーディオデータに加算する加算手段と、

前記設定手段より設定された前記モードと、前記検出手段により検出された前記 ID に対応して、前記類似ランダム系列の前記加算手段への供給を制御する制御手段とを備えることを特徴とするデスクランブルシステム。

【請求項 4】 前記類似ランダム系列を生成するための

初期値を、前記検出手段により検出された前記 ID に対応して修整する修整手段をさらに備えることを特徴とする請求項 3 に記載のデスクランブルシステム。

【請求項 5】 パケットを単位として伝送するビデオデータとオーディオデータの少なくとも一方を、前記パケットを単位としてスクランブルするスクランブル方法において、

前記パケットに含まれるデータが、前記ビデオデータまたはオーディオデータであることを表す ID を検出し、前記ビデオデータをスクランブルする第 1 のモード、前記オーディオデータをスクランブルする第 2 のモード、前記ビデオデータとオーディオデータの両方を同時にスクランブルする第 3 のモード、前記ビデオデータとオーディオデータを選択的にスクランブルする第 4 のモードのうちの少なくとも 2 つのモードの 1 つを選択的に設定し、

類似ランダム系列を発生し、

前記発生手段の出力する前記類似ランダム系列を前記ビデオデータまたはオーディオデータに加算し、

設定された前記モードと、検出された前記 ID に対応して、前記類似ランダム系列の前記加算手段への供給を制御することを特徴とするスクランブル方法。

【請求項 6】 パケットを単位として伝送されるとともに、前記パケットを単位としてスクランブルされているビデオデータとオーディオデータの少なくとも一方をデスクランブルするデスクランブル方法において、

前記パケットに含まれるデータが、前記ビデオデータまたはオーディオデータであることを表す ID を検出し、前記ビデオデータをデスクランブルする第 1 のモード、前記オーディオデータをデスクランブルする第 2 のモード、前記ビデオデータとオーディオデータの両方を同時にデスクランブルする第 3 のモード、前記ビデオデータとオーディオデータを選択的にデスクランブルする第 4 のモードのうちの少なくとも 2 つのモードの 1 つを選択的に設定し、

類似ランダム系列を発生し、

前記類似ランダム系列を前記ビデオデータまたはオーディオデータに加算し、

設定された前記モードと、検出された前記 ID に対応して、前記類似ランダム系列の前記ビデオデータまたはオーディオデータへの加算を制御することを特徴とするデスクランブル方法。

## 【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、例えば映像、音声などのデジタルデータを放送衛星、通信衛星などを介して伝送するデジタル放送システムにおいて、デジタルデータをスクランブルまたはデスクランブルする場合に用いて好適なスクランブルシステムおよび方法、並びにデスクランブルシステムおよび方法に関する。

## 【 0 0 0 2 】

【従来の技術】契約放送においては、スクランブル放送と呼ばれる放送方式が用いられることが多い。このスクランブル放送は、放送局側において、元信号を所定の方法で意図的に乱すことにより、放送局と契約していない者が放送を受信しても、正常な画像や音声データなどを利用することが出来ないようにするものである。放送局と契約した者に対しては、デコーダを与え、このデコーダによりスクランブルされているデータを元の形にデスクランブルすることで、正常な画像、音声データなどを得ることが出来るようにする。

【 0 0 0 3 】スクランブル放送においては、契約をしていない者に放送が受信された場合においても、その内容を知られないようにするために、出来るだけデスクランブルすることが困難な方法でスクランブルすることが望ましい。

【 0 0 0 4 】スクランブルの方式は、大きく 2 つに分類される。1 つはストリームサイファであり、他の 1 つはブロックサイファである。

【 0 0 0 5 】ストリームサイファは、疑似ランダム信号を発生させ、この疑似ランダム信号を元信号にモジュロ 2 加算することにより、元信号をスクランブルする方法である。

【 0 0 0 6 】これに対してブロックサイファは、DES (Data Encryption Standard) のように、ブロック単位で元信号を区切り、各ブロックで複雑な処理を繰り返す方法である。

【 0 0 0 7 】ストリームサイファは、ハードウェア構成が簡単である利点を有する反面、解読されやすいという欠点を有している。これに対してブロックサイファは、解読されにくいという利点を有する反面、ハードウェア構成が複雑になるという欠点を有している。

【 0 0 0 8 】ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission) 13818-1 (MPEG2 Systems) では、トランスポートパケットを単位として、マルチメディアのデータを多重化して伝送することが標準化されている。このパケットは 188 バイトの長さを有しており、デジタル映像、デジタル音声、データ信号が、パケット単位で多重化されている。多重化を柔軟に行うためには、パケット単位でスクランブルが完結するようにした方が、以後の伝送系においてパケットの編集などを自由に行うことができるため好ましい。またその方が、パケットの脱落などに関しても影響が少ない。

【 0 0 0 9 】ところで放送衛星を介して伝送するデータをスクランブルする装置として、平成 5 年 6 月 21 日の「電気通信技術審議会答申」により、「諮問第 53 号「放送衛星によるデータ放送に関する技術的条件」のう

ち、伝送制御方式および有料方式ならびにファクシミリ、テレソフトウエア、静止画、文字 (基本)、時刻の各信号の技術的条件」として、図 7 に示すスクランブル装置が提案されている。

【 0 0 1 0 】スクランブルキーは、32 ビットの初期値と、4 ビットの修整制御値よりなり、初期値を初期値レジスタ 1 にロードされ、修整制御値は修整制御レジスタ 5 にロードされる。このロードはキー更新タイミングフラグ S C T が 1 のパケットのとき行われる。

【 0 0 1 1 】初期値レジスタ 1 は、32 段のフィードバックシフトレジスタにより構成されている。この初期値レジスタ 1 にロードされたデータは、下位ビットから上位ビットへシフト信号に対応してシフトが行われる。

【 0 0 1 2 】前のパケットの連続性指標 C I の値 (0 乃至 15 のいずれかの値をとる) が 15 で、当該パケットの C I の値が 0 であるとき、C I のキャリーが 1 とされる。C I のキャリーはそのほかの場合 (連続性指標が 15 のパケットから 0 のパケットへの変化以外の変化である場合)、0 となっている。この C I の値が 1 で、修整制御レジスタ 5 の出力 f 3 が 1 のとき、アンドゲート 10 が論理 1 を出力する。この論理 1 が、スクランブルキー更新タイミングフラグ S C T が 0 であるとき、すなわち初期値レジスタ 1 にロードが行われる以外のとき、アンドゲート 6 を介して、シフト信号として初期値レジスタ 1 に入力される。初期値レジスタ 1 は、この論理 1 のシフト信号に対応してシフト動作を行う。

【 0 0 1 3 】初期値レジスタ 1 より出力された 32 ビットの初期値は、初期値修整回路 2 に入力され、修整される。この修整は、修整制御レジスタ 5 の出力 f 0 乃至 f 2 と、デジタルデータを伝送する論理チャンネルを識別するための論理チャンネル識別 L C I 1、L C I 2 および連続性指標 C I をアンドゲート 7 乃至 9 で論理積して得た初期値修整データに対応して行われる。

【 0 0 1 4 】初期値修整回路 2 が出力する修整された初期値は、P R P S (Pseudo-random binary sequence: 疑似ランダム 2 値信号系列)、生成回路 3 に入力される。P R B S 生成回路 3 は所定のロード信号が入力されたとき、この修整された初期値をロードし、アンドゲート 11 を介して所定のシフト信号が入力されたとき、その修整された初期値をシフトして、P N 信号 (疑似ランダム信号) を生成する。この P N 信号はスクランブル識別フラグ S C F が 1 のとき、アンドゲート 4 を通過し、加算器 12 に入力される。加算器 12 はアンドゲート 4 から入力された P N 信号を、図示せぬ回路から供給されたパケットデータに加算し、暗号化されたパケットデータとして出力する。

【 0 0 1 5 】この装置を、上述した M P E G 2 Systems のトランスポートパケットのスクランブルに用いることが考えられる。

【 0 0 1 6 】

【発明が解決しようとする課題】しかしながら、従来のスクランブル装置においては、例えば、所定の番組のデータをスクランブルする場合、そのビデオデータをスクランブルするだけでなく、オーディオデータもスクランブルするようになされており、ビデオデータだけ、あるいはオーディオデータだけを独立にスクランブルすることができない課題があった。その結果、提供できる情報の状態が画一的となり、提供する情報に対応して、変化に富んだ状態で情報を提供することができない課題があった。

【0017】本発明はこのような状況に鑑みてなされたものであり、より変化に富んだ状態で情報を提供することができるようにするものである。

【0018】

【課題を解決するための手段】請求項1に記載のスクランブルシステムは、パケットを単位として伝送するビデオデータとオーディオデータの少なくとも一方を、パケットを単位としてスクランブルするスクランブル装置において、パケットに含まれるデータが、ビデオデータまたはオーディオデータであることを表すIDを検出する検出手段（例えば図3のID検出部22A）と、ビデオデータをスクランブルする第1のモード、オーディオデータをスクランブルする第2のモード、ビデオデータとオーディオデータの両方を同時にスクランブルする第3のモード、ビデオデータとオーディオデータを選択的にスクランブルする第4のモードのうちの少なくとも2つのモードの1つを選択的に設定する設定手段（例えば図1の制御回路83）と、類似ランダム系列を発生する発生手段（例えば図3のPRBS生成回路39と、発生手段の出力する類似ランダム系列をビデオデータまたはオーディオデータに加算する加算手段（例えば図3の加算器12）と、設定手段により設定されたモードと、検出手段により検出されたIDに対応して、類似ランダム系列の加算手段への供給を制御する制御手段（例えば図3のANDゲート4）とを備えることを特徴とする。

【0019】類似ランダム系列を生成するための初期値を、検出手段により検出されたIDに対応して修整する修整手段（例えば図3の初期値修整回路2）をさらに備えることができる。

【0020】同様の構成によりデスクランブルシステムを構成することもできる。

【0021】請求項5に記載のスクランブル方法は、パケットを単位として伝送するビデオデータとオーディオデータの少なくとも一方を、パケットを単位としてスクランブルするスクランブル方法において、パケットに含まれるデータが、ビデオデータまたはオーディオデータであることを表すIDを検出し、ビデオデータをスクランブルする第1のモード、オーディオデータをスクランブルする第2のモード、ビデオデータとオーディオデータの両方を同時にスクランブルする第3のモード、ビデ

オデータとオーディオデータを選択的にスクランブルする第4のモードのうちの少なくとも2つのモードの1つを選択的に設定し、類似ランダム系列を発生し、発生手段の出力する類似ランダム系列をビデオデータまたはオーディオデータに加算し、設定されたモードと、検出されたIDに対応して、類似ランダム系列の加算手段への供給を制御することを特徴とする。

【0022】同様の構成によりデスクランブル方法を実現することができる。

10 【0023】

【作用】請求項1に記載のスクランブルシステムおよび請求項5に記載のスクランブル方法においては、4つのモードのうち、設定されたモードと、検出されたIDに対応して、類似ランダム系列のビデオデータまたはオーディオデータへの加算状態が制御される。したがって、ビデオデータだけあるいはオーディオデータだけをスクランブルしたり、両方を同時にスクランブルしたり、両方を交互にスクランブルしたりすることができ、より変化に富んだ状態を実現することができる。

20 【0024】請求項3に記載のデスクランブルシステムおよび請求項6に記載のデスクランブル方法においては、変化に富んだ状態でスクランブルされたデータを確実にデスクランブルすることが可能となる。

【0025】

【実施例】図1は、上述したISO/IEC 13818-1 (MPEG2 Systems) で規定するトランスポートパケットをスクランブルする本発明のスクランブルシステムの構成例を表している。暗号化される前のパケットデータは、スクランブル装置81に入力され、スクランブルされた後、暗号化されたパケットデータとして出力されるようになされている。入力部82を操作して、第1のモード乃至第4のモードのうちのいずれか1つのモードを指令すると、制御回路83は、その指令されたモードに対応する制御信号をスクランブル装置81に出力する。そして、スクランブル装置81は、入力された制御信号に対応して、スクランブル動作を行うようになされている。

【0026】スクランブル装置81（後述する図3のID検出部22A）は、制御回路83よりビデオデータだけをスクランブルする第1のモードの制御信号が入力された場合、検出したパケットIDがビデオパケットであることを表すとき、スクランブルすべきパケットであることを表すSCF信号をANDゲート4（図3）に出力する。

【0027】同様に、オーディオデータだけをスクランブルする第2のモードの制御信号が入力された場合、オーディオデータであることを表すIDパケットが検出されたとき、SCF信号を出力する。ビデオデータとオーディオデータの両方を同時にスクランブルする第3のモードの制御信号が入力された場合においては、ビデオデ

ータのバケットIDが検出されたとき、SCF信号を出力するだけでなく、オーディオデータのバケットIDが検出されたときもSCF信号を出力する。

【0028】これに対して、ビデオデータとオーディオデータを選択的にスクランブルする第4のモードの制御信号が入力された場合においては、図2に示すように、任意の数の連続するビデオバケットと、それに隣接する任意の数のオーディオバケットを1つのサイクルとし、第*i*サイクルにおいて、ビデオバケットとオーディオバケットのうち、ビデオバケットを検出したときSCF信号を出力した場合においては、その次の*i*+1サイクルにおいては、ビデオバケットを検出したときSCF信号を出力せず、オーディオバケットを検出したときSCF信号を出力する。このように、各サイクル毎に交互にビデオバケットまたはオーディオバケットが検出されたときSCF信号が出力される(スクランブルされる)。

【0029】図3は、上述したISO/IEC 13818-1(MPEG2 Systems)で規定するトランスポートバケットをスクランブルする図1のスクランブル装置81の構成例を示すブロック図であり、図7における場合と対応する部分には同一の符号を付してある。すなわちこの実施例においても、初期値レジスタ1乃至加算器12の構成は、図7における場合と同様である。ただしこの実施例においては、アンドゲート7乃至10に、修整制御レジスタ5より信号が供給されるとともに、検出回路22より出力された信号が入力されるようになされている。

【0030】この検出回路22は、バケットのヘッダに含まれるバケットIDを検出するID検出部22Aと、バケットのヘッダに含まれるcontinuity-counter(継続カウンタ)を検出するCC検出部22Bを有している。

【0031】その他の構成は図7における場合と同様である。

【0032】初期値修整回路2は、例えば図4に示すように構成される。この実施例においては、アンドゲート7乃至9より入力される合計15ビットのデータg<sub>0</sub>乃至g<sub>14</sub>が接続マトリックス31において、32ビットのデータh<sub>0</sub>乃至h<sub>31</sub>に変換され、それぞれ(h<sub>0</sub>, h<sub>1</sub>), (h<sub>2</sub>, h<sub>3</sub>), ..., (h<sub>28</sub>, h<sub>29</sub>), (h<sub>30</sub>, h<sub>31</sub>)のように、2ビットを単位とするデータに区分され、それぞれ加算器32-1乃至32-16に供給される。加算器32-1乃至32-16には、初期値レジスタ1より供給された32ビットの初期値データb<sub>0</sub>乃至b<sub>31</sub>が、(b<sub>0</sub>, b<sub>1</sub>), (b<sub>2</sub>, b<sub>3</sub>), ..., (b<sub>28</sub>, b<sub>29</sub>), (b<sub>30</sub>, b<sub>31</sub>)のように、2ビットずつ区分されて、それぞれ加算器32-1乃至32-16に供給される。

【0033】加算器32-1乃至32-16は、入力された4ビットのデータからそれぞれ2ビットのデータ

(c<sub>0</sub>, c<sub>1</sub>), (c<sub>2</sub>, c<sub>3</sub>), ..., (c<sub>28</sub>, c<sub>29</sub>), (c<sub>30</sub>, c<sub>31</sub>)を生成し、これを修整された初期値としてPRBS生成回路3に出力する。

【0034】PRBS生成回路3は、例えば図5に示すように構成される。この実施例においては、初期値修整回路2の加算器32-1乃至32-16より出力された修整初期値c<sub>0</sub>乃至c<sub>31</sub>のうちc<sub>0</sub>乃至c<sub>7</sub>が、8段のシフトレジスタで構成されるフィードバックシフトレジスタ41に入力されている。また、c<sub>8</sub>乃至c<sub>18</sub>が、11段のシフトレジスタで構成されるフィードバックシフトレジスタ42に供給されている。さらにc<sub>19</sub>乃至c<sub>31</sub>が13段のシフトレジスタにより構成されるフィードバックシフトレジスタ43に供給されている。

【0035】フィードバックシフトレジスタ41は、入力c<sub>0</sub>乃至c<sub>7</sub>から、データd<sub>0</sub>乃至d<sub>7</sub>を生成し、このうちd<sub>0</sub>乃至d<sub>5</sub>を非線形ロジック44に出力する。フィードバックシフトレジスタ42は、データc<sub>8</sub>乃至c<sub>18</sub>からデータd<sub>8</sub>乃至d<sub>18</sub>を生成し、このうちd<sub>8</sub>乃至d<sub>13</sub>を非線形ロジック45に出力する。フィードバックシフトレジスタ43は、データc<sub>19</sub>乃至c<sub>31</sub>から、データd<sub>19</sub>乃至d<sub>31</sub>を生成し、このうちd<sub>19</sub>乃至d<sub>24</sub>を非線形ロジック46に供給し、d<sub>31</sub>を加算器48に出力する。

【0036】非線形ロジック44は、データd<sub>0</sub>乃至d<sub>5</sub>から1ビットのデータp<sub>1</sub>を生成し、非線形ロジック45は、データd<sub>8</sub>乃至d<sub>13</sub>からデータp<sub>2</sub>を生成し、非線形ロジック46は、データd<sub>19</sub>乃至d<sub>24</sub>からデータp<sub>3</sub>を生成する。

【0037】スイッチ47は非線形ロジック45が出力するデータp<sub>2</sub>が0であるとき、図中左側に切り換えられ、非線形ロジック44の出力p<sub>1</sub>を選択し、加算器48に出力する。また、非線形ロジック45の出力p<sub>2</sub>が1であるとき、図中右側に切り換えられ、非線形ロジック46の出力p<sub>3</sub>を選択し、加算器48に出力する。加算器48は、非線形ロジック44の出力p<sub>1</sub>または非線形ロジック46の出力p<sub>3</sub>と、フィードバックシフトレジスタ43が出力するデータd<sub>31</sub>との排他的論理和を演算し、1ビットのPN信号pとしてアンドゲート4に出力する。

【0038】検出回路22は、入力されるバケットデータからそのヘッダを抽出する。すなわち入力されるバケットデータは、図6に示すようなフォーマットとされている。1バケットの長さは188バイトとされ、その先頭の4バイトはヘッダ、残りの184バイトがデータ部とされ、そこに実データが配置されるようになされている。

【0039】ヘッダには、その先頭に8ビットの同期バイトが配置され、続く3ビットを挟んでさらにそれに続く13ビットはビデオデータ、オーディオデータなどを識別するバケットID(PID<sub>0</sub>乃至PID<sub>13</sub>)とさ

れている。そして一番最後の4ビットが、continuity-counter (継続カウンタ) の4ビットのデータCCT0乃至CCT3とされている。

【0040】検出回路22のID検出部22Aは、図6に示した13ビットのパケットIDPID0乃至PID13を検出し、PID0乃至PID4の5ビットをアンドゲート7に、PID5乃至PID10の6ビットをアンドゲート8に出力する。そしてPID11乃至PID13と、CC検出部22Bにより検出された継続カウンタのデータCCT0乃至CCT3のうちのCCT0よりなる4ビットがアンドゲート9に出力される。

【0041】検出回路22は、パケットヘッダのキー更新タイミングを検出し、キー更新タイミングフラグSCTをアンドゲート6に出力するとともに、制御装置83から指令されたモードに対応するパケットIDを検出したとき、スクランブル識別フラグSCFをアンドゲート4に出力する。

【0042】また、検出回路22は、データ部の先頭においてロード信号を出力し、それをアンドゲート11とPRBS生成回路3に出力する。さらに、データ部の先頭以外においては、シフト信号をアンドゲート11に出力する。

【0043】次にその動作について説明する。検出回路22は、データ部の先頭データに加算するPN信号がPRBS回路3より出力されるより前の所定のタイミングにおいて、初期値レジスタ1に、1のスクランブルキー更新タイミングフラグSCTを出力し、初期値レジスタ1に、図示せぬ回路から供給される32ビットの初期値a0乃至a31をロードさせる。

【0044】また、修整制御レジスタ5は、スクランブルキー更新タイミングフラグSCTが1であるとき、図示せぬ回路から供給される4ビットの修整制御値e0乃至e3をロードする。そしてその4ビットのデータをそのまま4ビットの出力f0乃至f3として出力する。

【0045】すなわち修整制御レジスタ5は、ロード時に次の演算を行う。

【0046】

【数1】

ロードのとき

$$\sum_{i=0}^3 f_i x^i \Leftarrow \sum_{i=0}^1 e_i x^i$$

【0047】アンドゲート10は、CC検出部22Bが検出する継続カウンタの4ビットの値のうち、CCT1が1であり、且つ修整制御レジスタ5の出力f3が1であるとき、1のシフト信号を出力する。このシフト信号はキー更新タイミングフラグSCTが0であるとき(先頭以外のとき)、アンドゲート6を通過し、初期値レジスタ1に入力される。初期値レジスタ1はこのシフト信号が入力されると、下位ビットから上位ビットへデータ

を1ビットづつシフトする。最上位ビットは最下位ビットへシフトされる。初期値レジスタ1を構成する32段のフィードバックシフトレジスタの生成多項式は、次式で表される。

$$【0048】G1(x) = x^{31} + x^{22} + x^1 + x + 1$$

【0049】入力される初期値a0乃至a31に対して、出力をb0乃至b31とすると、この初期値レジスタ1は、ロード時およびシフト時において次の演算を行うことになる。

【0050】

【数2】

ロードのとき

$$\sum_{i=0}^{31} b_i x^i \Leftarrow \sum_{i=0}^{31} a_i x^i$$

シフトのとき

$$\sum_{i=0}^{31} b_i x^i \Leftarrow (x \times \sum_{i=0}^{31} b_i x^i) \bmod G1(x)$$

【0051】一方アンドゲート7は、ID検出部22Aが検出する13ビットのパケットIDのうち、5ビットのPID0乃至PID4と、修整制御レジスタ5の出力f0の論理積を演算し、15ビットの初期値修整データg0乃至g14のうちの、g10乃至g14を生成する。アンドゲート8は、ID検出部22Aが出力するPID5乃至PID10と、修整制御レジスタf1との論理積とを演算し、g4乃至g9を生成する。さらにアンドゲート9は、ID検出部22Aが検出するPID11乃至PID13、およびCC検出部22Bが検出するCCT0の4ビットのデータと、修整制御レジスタ5の出力f2との論理積を演算し、g0乃至g3を生成する。

【0052】初期値修整回路2の接続マトリックス31は、アンドゲート7乃至9より入力される15ビットの初期値修整データg0乃至g14を、次の表1に示すテーブルにしたがって、データh0乃至h31の32ビットのデータを生成する。

【0053】

【表1】

出力	h <sub>0</sub>	h <sub>1</sub>	h <sub>2</sub>	h <sub>3</sub>	h <sub>4</sub>	h <sub>5</sub>	h <sub>6</sub>	h <sub>7</sub>
入力	g <sub>6</sub>	g <sub>0</sub>	g <sub>14</sub>	g <sub>8</sub>	g <sub>10</sub>	g <sub>4</sub>	g <sub>2</sub>	g <sub>12</sub>

出力	h <sub>8</sub>	h <sub>9</sub>	h <sub>10</sub>	h <sub>11</sub>	h <sub>12</sub>	h <sub>13</sub>	h <sub>14</sub>	h <sub>15</sub>
入力	g <sub>8</sub>	g <sub>2</sub>	g <sub>0</sub>	g <sub>10</sub>	g <sub>12</sub>	g <sub>6</sub>	g <sub>4</sub>	g <sub>14</sub>

出力	h <sub>16</sub>	h <sub>17</sub>	h <sub>18</sub>	h <sub>19</sub>	h <sub>20</sub>	h <sub>21</sub>	h <sub>22</sub>	h <sub>23</sub>
入力	g <sub>7</sub>	g <sub>1</sub>	"0"	g <sub>9</sub>	g <sub>11</sub>	g <sub>5</sub>	g <sub>3</sub>	g <sub>13</sub>

出力	h <sub>24</sub>	h <sub>25</sub>	h <sub>26</sub>	h <sub>27</sub>	h <sub>28</sub>	h <sub>29</sub>	h <sub>30</sub>	h <sub>31</sub>
入力	g <sub>9</sub>	g <sub>3</sub>	g <sub>1</sub>	g <sub>11</sub>	g <sub>13</sub>	g <sub>7</sub>	g <sub>5</sub>	"0"

【0054】加算器32-1乃至32-16は、接続マトリックス31の出力h0乃至h31と、初期値レジ



タ1の出力b0乃至b31を、2ビットと単位とする16のブロックに区分し、次式で示される加算演算を行い、得られた結果をc0乃至c31として、PRBS生

成回路3に出力する。

[0055]

[数3]

$$c_{i+0} = b_{i+0} \oplus h_{i+0}$$

$$c_i = b_i \oplus h_i \oplus (b_{i+0} \cap h_{i+0})$$

$$i = 0, 2, \dots, 30$$

ここで、 $\oplus$ は排他的論理和を、 $\cap$ は論理積を表す。

【0056】PRBS生成回路3は、初期値修整回路2の加算器32-1乃至32-16より出力された32ビットの修整初期値c0乃至c31のうち、c0乃至c7をフィードバックシフトレジスタ41に、c8乃至c18をフィードバックシフトレジスタ42に、そしてc19乃至c31をフィードバックシフトレジスタ43に、それぞれロードする。

【0057】フィードバックシフトレジスタ41は、8段のシフトレジスタで構成され、次式で表される生成多項式G2(x)に従い、入力c0乃至c7に対して、データd0乃至d7を生成する。

$$[0058] \quad G2(x) = x^8 + x^4 + x^3 + x^2 + 1$$

【0059】フィードバックレジスタ42は、11段のシフトレジスタにより構成され、次式で表される生成多項式G3(x)を用いて、入力c8乃至c18に対してロードのとき

$$\sum_{i=0}^{31} d_i x^i \Leftarrow \sum_{i=0}^{31} c_i x^i$$

シフトのとき

$$\sum_{i=0}^{31} d_i x^i \Leftarrow \{(x \times \sum_{i=0}^7 d_i x^i) \bmod G2(x)\}$$

$$\div \{(x \times \sum_{i=8}^{18} d_i x^i) \bmod (x^8 \times G3(x))\}$$

$$\div \{(x \times \sum_{i=19}^{31} d_i x^i) \bmod (x^{19} \times G4(x))\}$$

【0066】非線形ロジック44には、フィードバックシフトレジスタ41が生成したデータd0乃至d7のうち、6ビットのデータd0乃至d5が入力される。非線形ロジック44は、このデータd0乃至d5を入力とし、1ビットのデータp1を生成する。

【0067】同様に非線形ロジック45には、フィードバックシフトレジスタ42が生成するデータd8乃至d17のうち、d8乃至d13が入力され、非線形ロジック45は、このデータd8乃至d13から、1ビットのデータp2を生成する。

【0068】また、非線形ロジック46には、フィードバックシフトレジスタ43が生成するデータd19乃至d31のうち、d19乃至d24が入力され、非線形ロ

データd8乃至d18生成する。

$$[0060] \quad G3(x) = x^{11} + x^4 + 1$$

【0061】フィードバックシフトレジスタ43は、13段のシフトレジスタで構成され、次式で表される生成多項式G4(x)を用いて、入力c19乃至c31に対して、データd19乃至d31を生成する。

$$[0062] \quad G4(x) = x^{13} + x^4 + x^3 + x^2 + x + 1$$

【0063】データのシフトは各パケットのデータに対応するクロックを用いて、下位ビットから上位ビットに向けて行われる。

【0064】以上のフィードバックシフトレジスタ41乃至43におけるロードと、シフトの動作をまとめると次の式で表すことができる。

[0065]

[数4]

ジック46は、このデータd19乃至d24から1ビットのデータp3を生成する。

【0069】 $i = 0, 8, 19$ における6ビットの入力( $d_{i+0}, d_{i+1}, d_{i+2}, d_{i+3}, d_{i+4}, d_{i+5}$ )の(0, 0, 0, 0, 0, 0), (0, 0, 0, 0, 0, 1), (0, 0, 0, 0, 1, 0), ..., (1, 1, 1, 1, 1, 1)に対応する1ビットの出力pをそれぞれ、(p(0, 0, 0, 0, 0, 0), (p(0, 0, 0, 0, 0, 1), ..., p(0, 1, 1, 1, 1, 1), (p(1, 0, 0, 0, 0, 0), (p(1, 0, 0, 0, 0, 1), ..., p(1, 1, 1, 1, 1, 1))で表すものとする、非線形ロジック44乃至46の出力は、次のように表すことができるようにす

る。

【0070】非線形ロジック44

(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1,  
0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0,  
1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1,  
0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0,  
1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1,  
1, 1, 0, 1)

【0071】非線形ロジック45

(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 10  
1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1,  
0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1,  
1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1,  
1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1,  
0, 0, 0, 0)

【0072】非線形ロジック46

(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0,  
0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0,  
1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1,  
0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 20  
0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0,  
0, 0, 0, 1)

【0073】そして、非線形ロジック45の出力p2が0であるとき、スイッチ47は、非線形ロジック44の出力p1を選択し、加算器48に出力する。また非線形ロジック45の出力p2が1であるとき、スイッチ47は非線形ロジック46の出力p3を加算器48に出力する。

【0074】加算器48は、非線形ロジック44の出力p1、または非線形ロジック46の出力p3と、フィードバックシフトレジスタ43の出力d31との排他的論理和の演算を行い、1ビットのPN信号pを生成する。 30

【0075】すなわち、スイッチ47と、加算器48により、次の演算が行われることになる。

【0076】

【数5】

$$p = \{(p1 \cap \overline{p2}) \cup (p3 \cap p2)\} \oplus d31$$

ここで、 $\neg$ は否定、 $\cap$ は論理積、 $\cup$ は論理和、 $\oplus$ は排他的論理和を表す。

【0077】PRBS生成回路3が出力するデータpは、スクランブル識別フラグSCFが1であるとき（スクランブルすべきパケットであるとき）、アンドゲート4を介して、加算器12に供給され、パケットデータとの排他的論理和が演算されて、暗号化されたパケットデータとして出力される。

【0078】そして、検出回路22は、制御装置83を介して入力部82より入力されるモードに対応してSCF信号をアンドゲート4に出力する。その結果、第1のモードにおいてはビデオパケットだけが、第2のモード 50

においてはオーディオパケットだけが、第3のモードにおいてはビデオパケットとオーディオパケットの両方が、第4のモードにおいてはビデオパケットとオーディオパケットが交互に、それぞれスクランブルされる。

【0079】なお、上記実施例においては、PID0乃至PID13、およびCCT0、CCT1から初期値補正データを生成するようにしたが、この他、CCT2、CCT3を用いるようにすることもできる。

【0080】なお、データ部に記録される実データとしては、映像データ、音声データ、その他のデータの他、任意のデータとすることができる。

【0081】また上記実施例においては、スクランブル装置を説明したが、全く同様の構成により、デスクランブル装置を実現することができる。

【0082】

【発明の効果】以上の如く、請求項1に記載のスクランブルシステムおよび請求項5に記載のスクランブル方法によれば、第1のモード乃至第4のモードのうち、設定されたモードと検出されたIDに対応して、類似ランダム系列のビデオデータまたはオーディオデータへの加算を制御するようにしたので、より変化に富んだ状態で、ビデオデータまたはオーディオデータをスクランブルすることができる。

【0083】その結果、例えば音楽を中心とする番組においては、主要な情報であるオーディオデータはスクランブルするが、ビデオデータはスクランブルしないようにして、あえて画像をモニタさせることで、それに付随するオーディオを聞きたくなるようにさせたり、その逆に、例えば映画などのように、様々な画面における画像が中心となる番組においては、ビデオデータをスクランブルし、オーディオデータをスクランブルしないようにして、オーディオだけをモニタさせて、その番組に興味を持たせるようにすることができる。あるいはまた、局部的に（極めて短時間だけ）画像をモニタさせたり、音声をモニタさせることにより、その番組に興味を持たせるなどすることができる。

【0084】また、請求項3に記載のデスクランブルシステムおよび請求項6に記載のデスクランブル方法によれば、上述したスクランブルシステムおよび方法における場合と同様の効果を奏することができる。 40

【図面の簡単な説明】

【図1】本発明のスクランブルシステムの構成例を示すブロック図である。

【図2】ビデオパケットとオーディオパケットを交互にスクランブルする例を示す図である。

【図3】図1のスクランブル装置81の構成例を示すブロック図である。

【図4】図3の初期値修整回路2の構成例を示すブロック図である。

【図5】図3のPRBS生成回路3の構成例を示すプロ

ック図である。

【図6】トランスポートパケットのフォーマットを説明する図である。

【図7】従来のスクランブル装置の構成例を示すブロック図である。

【符号の説明】

- 1 初期値レジスタ
- 2 初期値修整回路
- 3 PRBS生成回路
- 5 修整制御レジスタ
- 21 キー切り換え回路

22 検出回路

2.2 A ID検出部

2.2 B CC検出部

31 接続マトリックス

32-1乃至32-16 加算器

41乃至43 フィードバックシフトレジスタ

44乃至46 非線形ロジック

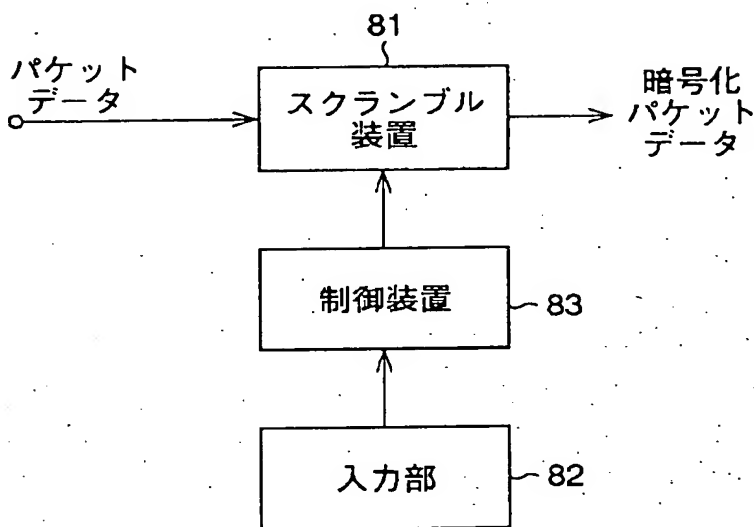
47 スイッチ

48 加算器

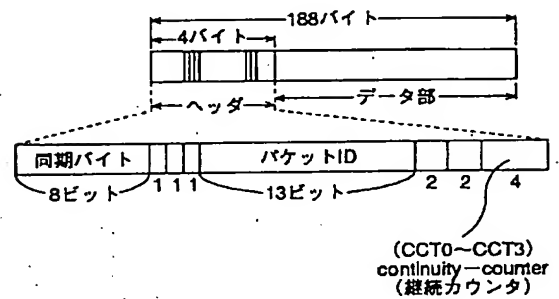
10 61, 62 キーレジスタ

63 セレクタ

【図1】

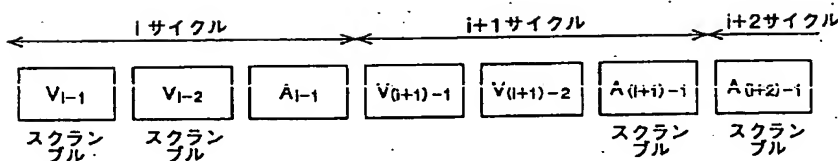


【図6】



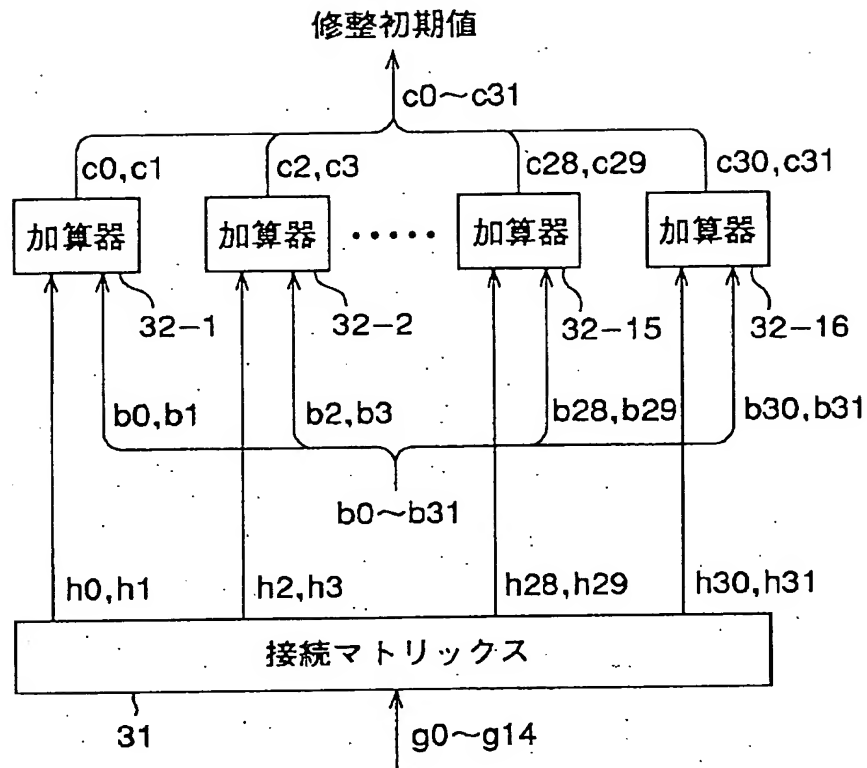
トランスポートパケット

【図2】

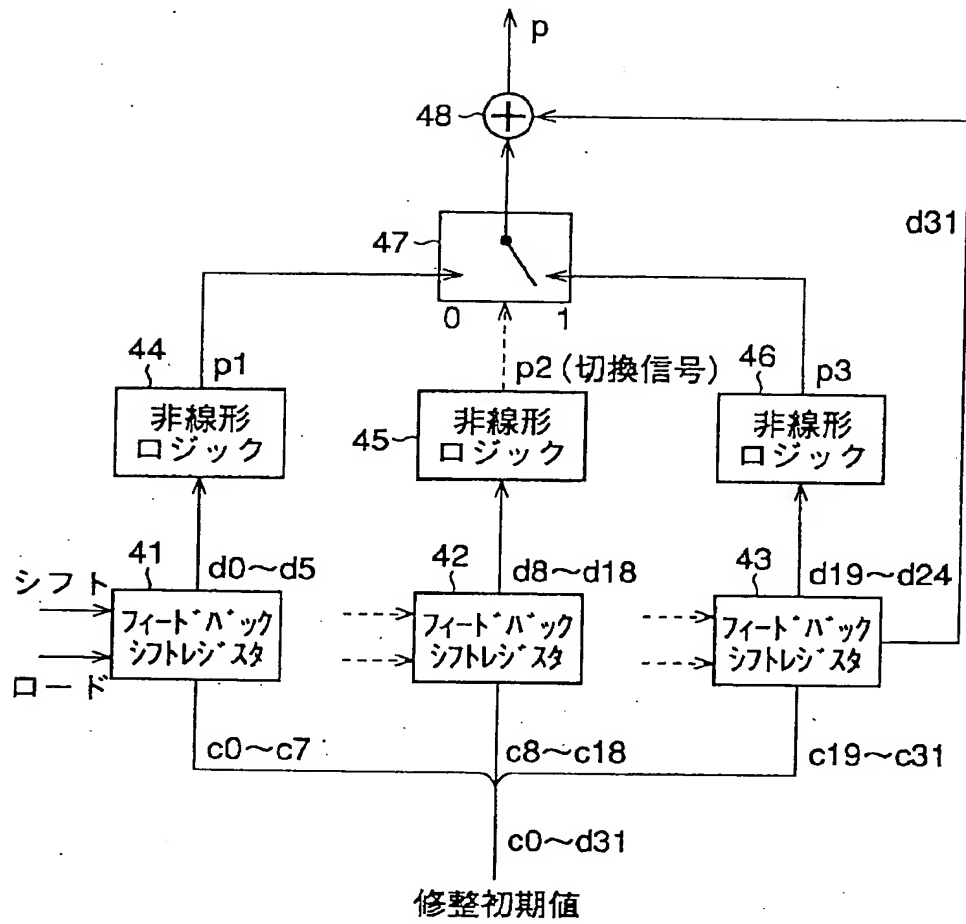




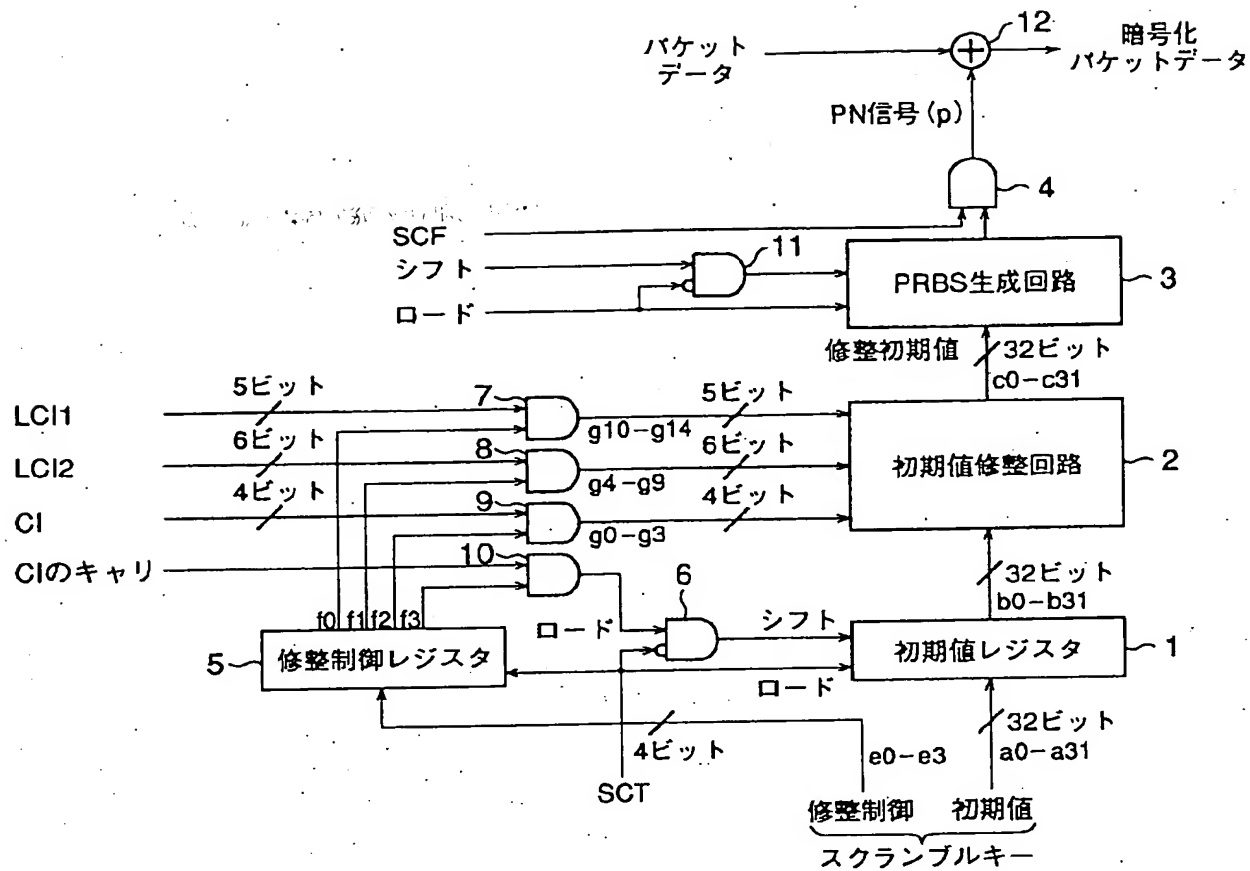
【図 4】

初期値修整回路 2

【図 5】

PRBS生成回路 3

【図 7】



フロントページの続き

### 技術表示箇所

H O 4 N 7/167

H O 4 N 7/167

**THIS PAGE BLANK (USPTO)**